MAGIC Meeting Minutes
November 20, 2013

Attendees

Jim Basney	NCSA
Rich Carlson	DOE/SC
Matt Chambers	Clemson
Billy Cook	Clemson
Rudi Eigenmann	NSF
Jill Gemmill	Clemson
Dan Gunter	LBL
Tom Hacker	Purdue
Dan Katz	NSF
Ken Klingenstein	Internet2
Mark Luker	NCO
David Martin	Northwestern U.
Grant Miller	NCO
Inder Monga	ESnet
Anita Nikolice	NSF
Lavanya Ramakrishnan	LBNL
Steve Teucke	U. Chicago
Harold Teunissen	SurfNet
Kevin Thompson	NSF

Action Items
1. Continuing: Grant Miller should approach Jim Bottom of Clemson U. to discuss the results of his workshop on Identity Management.

Proceedings

This MAGIC Meeting was chaired by Rich Carlson of DOE/SC and Dan Katz of the NSF. Several participants discussed Identity Management with an international context including:

- Steve Tuecke
- Jim Basney
- Harold Teunissen
- Ken Klingenstein

The identity challenge in science: Steve Tuecke

Developers of collaborative science tools need to: Assign identities to users, manage user profiles, and organize users into groups. High-quality 9implementations of this are difficult leading to identity "islands" across science domains and projects. Globus Nexus is a custom web application to streamline collaborative tool development. It provides identity, group, and profile management. Nexus provides:

- Identity provisioning: creating and managing Globus identities
- Identity hub: Link with other identities to authenticate to Nexus

- Group hub: User-managed group creation and management
- Profile management: User-managed profile attributes and visibility

Globus Nexus can then be used as an identity provider (IDP) for a project for user management, email, validation and other services. DOE's System Biology Knowledge Base (kBase) is an example.

Identity hub links identities form other federated IPPs with a Nexus identity, such as InCommon (SAML), Google (OpenID), XSEDE (OAuth, MyProxy), IGTF-certified X.509 CA, SSH. The linked identity can be used to authenticate to the Nexus identity. The Nexus federated IDP can leverage 3rd party services. Nexus has cache delegated credentials (X.509, via CILogon, MyProxy).

Globus Online manages identities including Openid (google.com), Myproxy (grid.ci.uchicago.edu), ssh2 (SSH Public Key), x.509 (Globus C), and Oauth (CILogon)

As an example, a user creates a Biomedical Informatics Research Network (BIRN) ID. The user links campus ID and XSEDE ID. Then the user can:

- Authenticate to BIRN with campus ID
- Query catalog (Nexus/BIRN ID)
- Request data transfer from BIRN to campus
- Request transfer from BIRN to XSEDE

The Group Hub provides user-managed group creation and management, flexible control over admission policies and visibility, and groups can be used in authorization decisions.

Globus/Nexus currently has 12,000 users and about 5,000 linked identities. It has 557 groups; the largest group has 402 members (kBase).

User profiles are sets of attributes/values of a user (e.g., name, email, address, field of science,…). Profile attributes can be self-asserted (name), validated (email, linked identity) or asserted by another user. Sources of profile attributes include social sites, campus Shibboleth servers and Nexus users. There is a proposal to replace current and ad hoc systems with Globus Nexus identity and group service.

The complete briefing is posted on the MAGIC Web site at:
http://www.nitrd.gov/nitrdgroups/index.php?title=Middleware_And_Grid_Interagency_Coordination_(MAGIC)#title

CILogon: Jim Basney

CILogon provides personal digital certificates for access to cyberinfrastructure. It uses federated authentication for user identification. The user logs on to CILogon using their campus (InCommon) or Google (OpenID) account. CILogon bridges InCommon and IGTF. It provides a translating mechanism and policy across higher education and grid trust federations. It provides multiple levels of assurance.

- CILogon Silver CA is accredited by IGTF
- IGTF IOTA profile for CILogon Basic is under development
- Google Authenticator support for second authorization factor

CILogon is integrated with cyberinfrastructure, with Globus Nexus, and it is used by OSG Connect. It is integrated with DOE KBase. Ligo uses ligo-proxy-init using the CILogon ECP. CILogon is a component of the XSEDE architecture and XSEDE can provide sustained operational support to CILogon users. To add and identity profile to CILogon use their Web self-service at: https://cilogon.org/requestidp/

The InCommon research and scholarship program helps services connect with identity providers. CILogon certificates issued include OAuth, ECP, PKCS12, and JWS.

CILogon is working toward SAML interfederation (InCommon is joining eduGAIN this year and international attributes are being released this year. CILogon is seeing growth of federated on-line CAs and levels of assurance are being strengthened:

- IGTF IOTA profile
- International adoption of Kantara standards
- Security incident handling
- Multi-factor authentication

The complete briefing is posted on the MAGIC Web site at:
http://www.nitrd.gov/nitrdgroups/index.php?title=Middleware_And_Grid_Interagency_Coordination_(MAGIC)#title

SURFNet Identity Management: Harold Teunissen

SURFNet identity management uses federated identity management based on SAML. The attribute provider is the new identity provider. Also included are certificate services, certificate transparency, open collaboration exchange_ Federation of federations, and other capabilities. Multi-disciplinary collaborations are enabled and will become increasingly common.

OpenContext provides middleware to make campus, cloud bzsed services and resources usable for collaboration both inter-campus and in virtual collaborations. OpenContext provides the Identity and Group Infrastructure and offers the platform software to run your own large collaborations. OpenContext facilitates international collaborations and virtual organizations. It facilitates global interconnection of IdPs and SPs. It provides a harmonizing attribute exchange that enlarges the SPs that access IdPs. Ideally for any participating countries, SPs and IdPs will have to provide OpenContext information only once. It is an add-on to EduGAIN. For individual SP-IdP cases the eduGAIN policies might need to be reinforced with bi-lateral agreements. OpenContext invites NRENs to work out organizational, technical, and policy/legal issues on a continuing basis.

The complete briefing is posted on the MAGIC Web site at:
http://www.nitrd.gov/nitrdgroups/index.php?title=Middleware_And_Grid_Interagency_Coordination_(MAGIC)#title

Upcoming Meetings

OSG and XSEDE are offering a summer school to provide understanding of the principles, concepts and applications. A link to this meeting is provided on the XSEDE Web page.

Next MAGIC Meetings

- January 8, 2014, 2:00-4:00 EST, NSF, Room II-415
- February 5, 2014 2:00-4:00, NSF, Room II-415